SOLITAIRE INTERGLOBAL LTD

Navigating Thru Chaos

Pervasive Encryption – A Summary

A New Paradigm for Protection

I've been a professional hacker for more than 15 years. I find cybersecurity problems in technology in order to make that technology more secure. But after doing this for many years, I'm frustrated. I see the same problems over and over again. We are not getting better. And while we depend more and more on technology, technology is becoming more and more insecure."

– Cesar Cerrudo, professional hacker, and CTO of IOActive Labs

---

Read full paper >

All of cyberspace and its underlying infrastructure is vulnerable to a wide range of risk and exposure from both physical and cyber threats and perils. Sophisticated cyber individuals and groups exploit standalone and congregated vulnerabilities to steal money and information, or disrupt, endanger and damage operations. The combination of wide opportunity for crime in cyberspace and the ability to execute from geographically-dispersed locations has produced a transformation of traditional criminal activities.

Cyberspace is extremely difficult to secure. The increasing integration between cyberspace and the physical world has exponentially expanded the opportunities for theft, damage and corruption. Reducing vulnerabilities and minimizing consequences in complex cyber networks are the goals, but ones that are increasingly difficult to achieve. The basic approach to security is proving to be inadequate to the demands of the aggressive nature of the environment. A paradigm shift is necessary and soon.

Research data was compiled by Solitaire Interglobal, Ltd. (SIL). Information from organizations concerned with the effectiveness of their security form the base study data, supplemented by threat and security information from the Global Security Watch (GSW) whose main focus is the impact on business operation, organizational assets, and prevention and remediation costs. This analysis examined the real-world impact on business security based on platform architecture. For that purpose, metrics for major architectures such as IBM's z Systems platforms, UNIX and x86 products were compared. A few of the highlighted findings can be seen in the quick summary below.

180 South Western Avenue, #275
Carpentersville, IL 60110
Phone (847) 931-9100 Website www.sil-usa.com

The current release of the IBM Z platform has a substantial advantage in terms of TCO, performance, and risk compared to the other platform options on the market today. The current level of available selective encryption and the resistance of the native platform to common threat vectors provide organizations with a significant foundational safeguard.

The advent of pervasive encryption radically changes not only the safeguard that's available on the Z offerings but the industry in general. This paradigm shift is a challenge to any other offering that tries to address business today.

Summary of Findings

Quick Summary

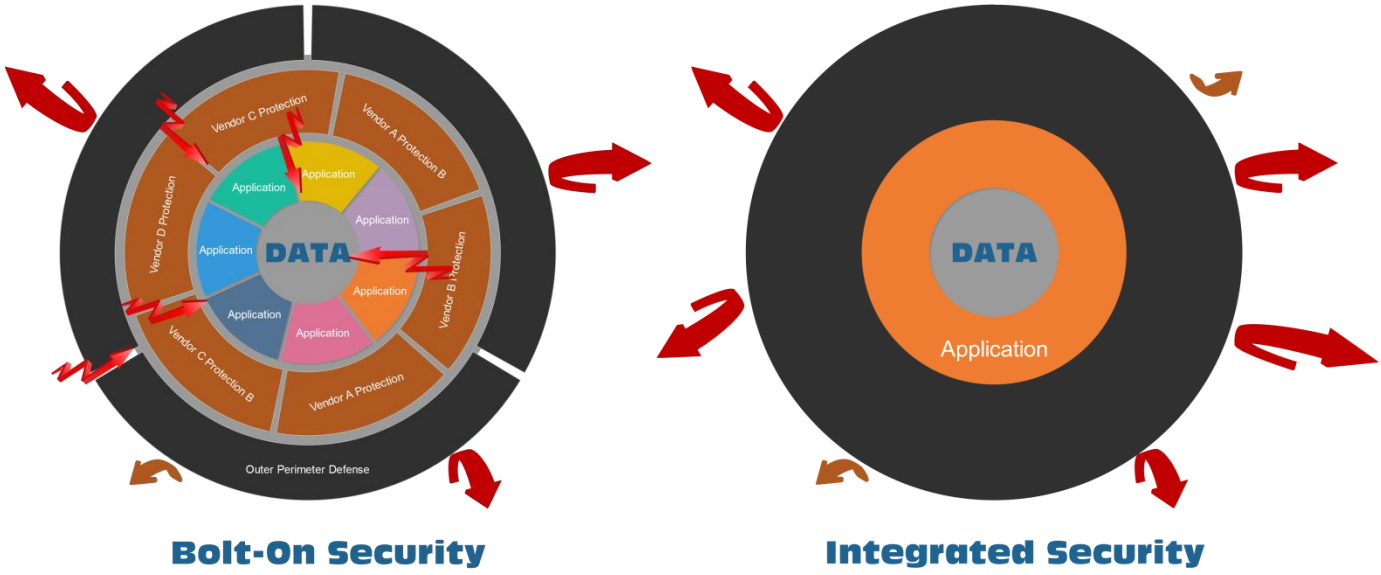
Category	Commentary	Quick Byte
Speed of Response	The same standard activities on Z consume up to ***85.80% less*** clock time than those executed on other platforms.	Faster security response is delivered by Z.
Risk	SIL risk profiling sets the Z platform risk rating at ***less than 1/20*** of any of the alternative solutions.	The security risk is significantly lower when deploying on Z platforms.
Security Effectiveness	Based on initial installations, the foundation Z security solution provides ***as much as 8.5 times*** the interception level of alternative platform solutions at ***93% less*** cost in overall expenditure, and with ***81% less*** effort.	IBM Z platforms provide the most secure application environments.
Security Effectiveness	The Z platforms deliver base incursion interception that is ***as much as 20.74%*** better than the alternate platform solutions with fully augmented security.	The base security delivered by Z platforms is more effective than the augmented solutions on alternate platforms.
Staff Effort	Time and motion studies show that Z security solutions require ***81% fewer tasks*** to implement standard protection levels.	IBM Z requires less staff effort to secure.
Remediation	Remediation costs on Z security deployments average **98.82% less** than the alternative platforms.	Repairing security damage is less expensive on Z.

Category	Commentary	Quick Byte
Total Cost of Security Ownership	The TCO for Z security implementations is lower by ***as much as 83.72%*** than for those of other platforms.	Your security expense dollars bring you more on a Z.
Total Cost of Information	The IBM Z implementations show as much as ***84.83% lower*** TCI over a wide range of organization size.	Working with your information on Z is less expensive.
Pervasive Encryption	IBM mainframe architecture can deliver encryption up to ***18.4 times faster***, for ***only 5%*** of the cost of other platform solutions.	Pervasive encryption changes the game.
Risk Mitigation Funding	An organization with an IT budget of $12M would see a difference in required set asides of $764,400 for x86 versus $160,524 for IBM Z.	Lower risk on a Z translates into less financial set-aside for cyber insurance.
Uniqueness	At this point in time, IBM Z is the only architecture that can support the pervasive encryption model.	Protect your IT assets now.

Extended periods of active incursion presence can have a substantial negative effect on organizational viability. Business stands to suffer between 16.2%-63.7% average reduction in gross revenues and valuation if an incursion lasts longer than three months.

When tactical responsiveness includes the addition of layers of security and safeguarding, the resulting architecture starts to resemble an onion with layers to provide additional safety. However, the actual layers themselves can create additional points of assailable topology.

Each place that a partial solution is “bolted onto” is yet another target for a knowledgeable hacker. The more complex layers allow the assailable topology to be higher. This vulnerability is part of a security risk profile that is increasingly used by insurance companies to determine the exposure of an organization to significant cyber damage.



Additional stress on security is created by the increased use of virtualization software. Each of those virtual machines creates new points of vulnerability and adds to the complexity of the security challenge. This significant difference stems from the base structure and realized strategy behind the platform architecture, chip design, operating system, and method of stack integration.

It is not only the number of attacks that has changed. The face of the incursions themselves has significantly changed.

One of the fastest growing threat vectors is the ransomware attack. In this type of attack, the incursion locks the files, directories, and other components of the system. The owner is asked to pay for an unlock code, which may or may not actually work.

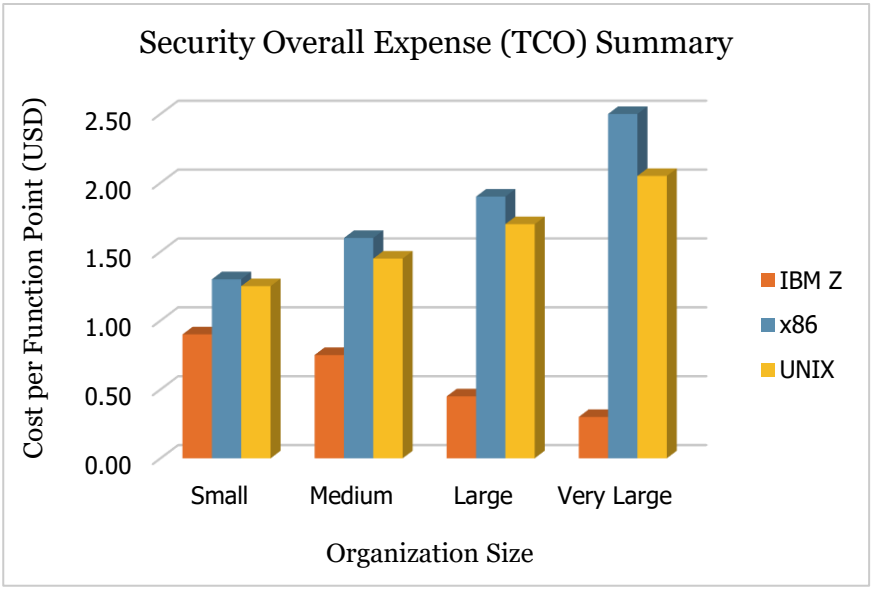
Security measurement is reflective, as it is evaluated by the absence of pain and problems. Security failure is highly visible, while its success is invisible. The study has been primarily directed at the value of security from a business perspective, so that those whose role it is to provide business leadership can understand the benefit of the IBM Z security offerings with pervasive encryption when evaluating security solutions.

In the collection and analysis of the study data, a number of characteristics were derived. These characteristics affect the overt capacity, efficiency, and reliability of the secured environment. Also examined was the synergy of security and business operations. The business perspective encompasses a myriad of factors, including reliability, degrees of security, staffing levels, total security cost (including recovery) and other effects. These tie directly into the decisions that IT managers, CTOs, and business leadership have to make daily.

Total Cost of Ownership

The total cost of ownership (TCO) provides one of the main business side metrics for operational efficiency. Once again, the projects and their expenditures have been normalized based on the standard basis enabling large and small organizational expenditures to be more accurately compared.

The patterns of expenditures show increasing trends for some of the platform types as the complexity of the deployment grows. There is a contradictory trend for IBM Z. A declining pattern of unit expenditure translates into the efficiency of scale, where the leveraging of framework and foundation allows a cost-efficient pattern of financial investment. As seen in the following chart, the expenditures for Z security implementations are ***lower by as much as 83.72%*** than for those of other platforms. This stems partially from the combination of architected security base and highly scalable platform.



> "Our IBM mainframe has a much lower cost than any of the other things we do as a company. The costs have actually gone down over the last three years, although our financial people keep telling us that the costs are too high. I keep telling them that the overall cost is lower since we have fewer problems, fewer staff, and less chance of problems."
>
> CFO - Very Large Distributer

In situations where security is handled with a series of additive protection components or where main security governance is solely resident in the deployed application, the overall expense comparison takes a significant jump when new services are added. The following chart shows this type of effect. The projects included in this portion of the analysis show the short-term impact of security acquisition. In all cases, these 16,027 organizations added a single cloud application to existing cloud deployments. The deployments targeted private, public and hybrid clouds and were designed for more than 1K users.

Communicating the actual cost and impact of security is another challenge. The articulation of a business case for security improvements and expansion is a frequent topic of discussion and an object of complaint by security professionals all over the world. The cost impact of security as an aspect of operational efficiency is not clearly understood by the majority of business executives. In a pool of data collected in 2015-16 that included over 9.5 million organizational executives, less than 11% had ever seen a business case for security expenditures. Less than 0.9% of these people claimed to understand how security costs, economies of scale and projected expenses were derived. Sadly, less than 35% of the people responsible for making strategic organizational decisions believed that their security personnel understood how to project or calculate costs. All of these contribute to a situation where the reduction, or increase, of overall security workload cost allocations are unexpected and unappreciated. With this particular blind spot, executive management fails to understand the sizable efficiency of IBM Z security deployments.

Security Effectiveness

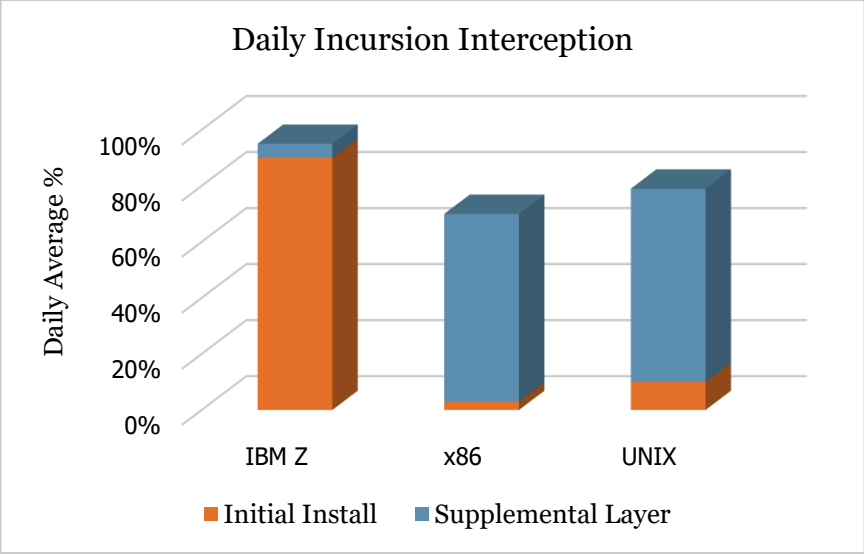
To examine the area of security effectiveness, SIL found measurable comparisons in a combination of objective and subjective metrics. The objective metrics included the ability of the security measures to capture and prevent successful incursion, both in the reported incursions and those discovered by detail audits. The information contained in this measurement has applicability to both the technical side and business side of an organization since the quantity of incursions can be largely translated into the effect on the organization's bottom line.

Each of these areas provides some key differentiation for the IBM Z cyber security solution.

Incursion Resistance

The primary metric of security success is the number of incursions that are trapped, neutralized or prevented from causing any form of damage. The incursions aggregated into this metric do not include those incursions that have been blocked by add-on firewalls and security devices. Instead, only those blocked by the security solution present on the platform have been counted.

The level of incursion blocking provided by the initial installation for each of the platforms forms the foundation for any add-on security required or installed. The graph below shows the security provided by the initial installation and the supplemental layer, expressed as a percentage of incursions that have been blocked. Based on initial installations, the foundation IBM Z security solutions provide as much as 13.21 times the interception level of alternative platform solutions. Additionally, the Z solution provides a base, foundational protection that ***exceeds 92.1%,*** even without the bolt-on supplementation required for alternate architectures.



Supplemental security layers are add-on applications, tactics, and techniques, etc. These differ from organization to organization but are variable based on individual security oversight, posture, and governance. Higher levels of supplemental security requirements indicate increased levels of effort on the part of security software and personnel.

The combination of intellectual capital and automated services, coupled with the architectural design of the IBM Z cyber security solutions, results in the interception of a significantly higher percentage of incursions. The Z platform delivers base incursion interception that is as much as ***20.74% better*** than the combined security of foundation augmented with extensive, competent and rigorous efforts for supplemental security tactics, techniques and procedures provided by other alternate platform solutions.

> "I have no idea exactly why there are fewer security problems with the z *(sic)* platform, I simply know that we don't have any. The security people are constantly telling me things about this and that, it really boils down to it just works. The last time we had a problem with security on that platform it turned out that somebody stole somebody else's password. The last time I had a problem on a different platform was about an hour ago. Ask *(sic)* me which would *(sic)* I would prefer!"
>
> CIO - Large Distributor

The nature of embedded Z security is significantly different than that which is created with additive protection solutions. With a broader group of interfaces to secure, the protection of the organization's data and process is most vulnerable when defined at the device level. A more effective strategy pulls the policy control and definition to a more centralized point. The highly integrated and embedded Z security stack provides a significant advantage in this area.

Security Risk Factors

Security risk can be defined as the potential that a given threat will successfully exploit vulnerabilities of a process or an asset or group of assets, causing harm to the organization or the clients it serves. It is measured in terms of a combination of the probability of occurrence of such an event and its associated consequences. SIL builds risk profiles that are actuarial constructs used to provide a consolidated view of the overall risk of an organization. This incorporates individual risk contribution from applications, interfaces, management structures, social engineering aspects, etc.

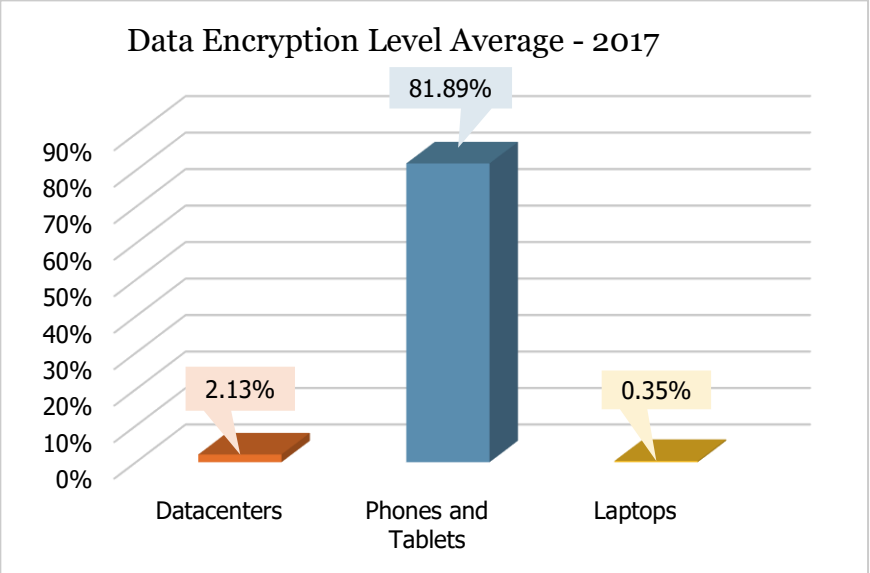
> "A variety of attacks have left us reeling from customer fade, remediation costs, and other horrific influences. The whole experience has resulted in a big loss of customer confidence. We are moving quickly to an MSP that runs some of the workload on a big mainframe, since that seems to the only safe place to run these days."
>
> Director - Medium Distribution Company

Pervasive Encryption

An organization's client and corporate data is a key resource. It is literally priceless since it forms the core market advantage and intellectual capital of any business. Encryption has been one way of protecting this asset since once encrypted, its availability and vulnerability to hackers is destroyed. Many of those assets are currently unprotected.

The perspective is different in other areas of data communications. The use of mobile devices has been built on a view of privacy that included encryption from the initial design onward. A comparison of the different encryption levels is enlightening.

This summary highlights the base difference in the mainstream IT and mobile communications approach. Since the communication industry realized early on the importance of encryption when it came to mobile devices, approximately 82% of data on those platforms is encrypted. The discordance of the lack of encryption on the extremely valuable organizational resources located in datacenters and on laptops is severe.



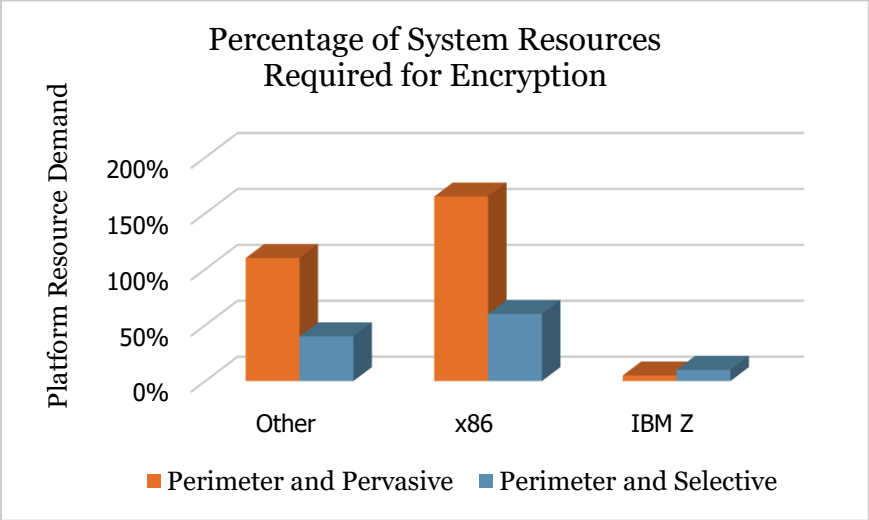
There are several core reasons for the low levels of encryption. The cost in terms of time and system capacity has encouraged organizations to concentrate on perimeter defense techniques and selective encryption. With increasing demand for perimeter security defense consuming ***up to 61.2%*** of alternate platform capacity, a paradigm shift is indicated. A recent advance in one of the foundational aspects of our current computing environment is poised to make a significant difference in the market. The change is the expansion of the current IBM Z encryption from a selective model to one that is pervasive. Such a significant modification in the basic structure of computing and its effect on security will cause a major disruptive effect.

The overall concept is to not introduce a decision layer that says what will or will not be encrypted. Instead, it will be possible to have encryption be part of normal processing. The removal of the decision for selective encryption is a further savings in the overall cost and a reduction in the difficulty in using encryption in the current market.

The largest barrier to doing full-scale encryption has been the cost of the encryption and the performance load that such activity puts on the computing platform. However, the bolted-on solutions that are being deployed have grown in capacity demand until there are ***loads of up to 61%*** of the system load that is being consumed by security processes in the reporting organizations. That translates into a significant amount of infrastructure costs, performance drags, etc.

The current encryption resource requirements can be clearly seen in the chart above. Even without the newest advances, the Z architecture delivers encryption with more effective and less costly resource expenditure. It delivers ***over 8.5 times*** the security protection, at ***93% less cost*** in overall expenditure, and with ***81% less effort***. This is, however, selective encryption which lessens some of the desperately needed protection.

The full impact of the faster encryption engine and the ability to encrypt information in bulk creates a fully pervasive solution that runs more than ***18.4 times faster*** and at only ***5% of the cost*** of other solutions.



Although pervasive encryption is feasible on the Z mainframe, it is not currently possible to implement on other architectures. The most restrictive of the architectures, tied to the x86 solutions, would require ***7.32 times*** the current capacity to execute the workload necessary for pervasive encryption on a single server. Using the average per architecture within the study group, that translates into ***12.2 times*** the number of platforms currently installed at those sites. Otherwise, the requirements for this type of solution will require significant advances in those alternate platform chip design, operating system foundation, and other internal platform capacity restrictions. Such advances are long term changes in chip design and manufacturing, with typical lead times of 2-3 years, assuming that the base technology can be created.

If that is not done, then the demands of pervasive encryption cannot be met on those platforms. The systems that are resident on those platforms will continue to run with higher risk and exposure profiles, demand an excessive amount of personnel time and expenditure and consume disproportionate amounts of organizational resources.

Applying encryption in a pervasive layer would significantly reduce the percentage of the platform that has to be devoted to the security processes themselves. For the analyzed organizations in a recent SIL study, the ***reduction would be as much as 91.7%***.

Workload and speed of response are very important when it comes to security. In the comparison of selective versus pervasive encryption within that same study, ***87.2% more*** of the incursions were handled automatically by the pervasive model.

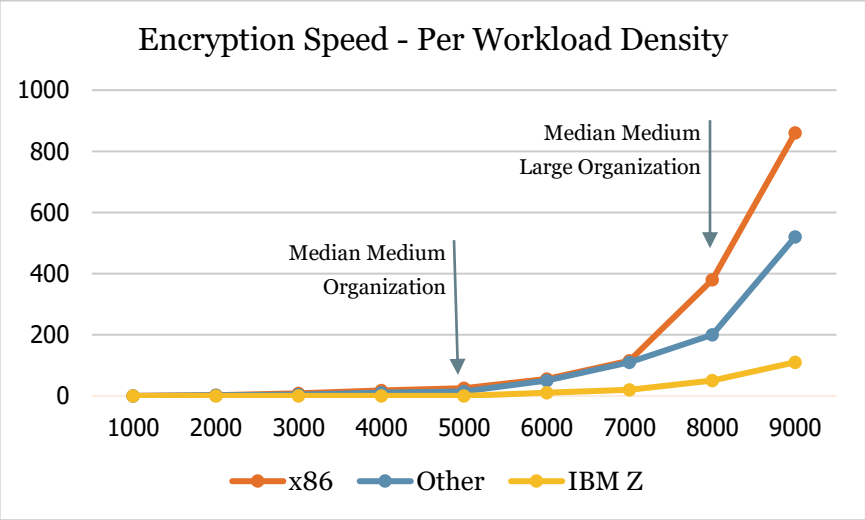
For those that required a response, the speed of the response was much faster on the pervasive side. In the tests, the speed of response ***required only 14.2%*** of the time required for the selective encryption response.

Assailable topology is also reduced. With fewer assailable layer points, threats can be addressed in a more comprehensive and less complex fashion. This lower complexity also could significantly reduce the risk of future hacks. The assailable topology went from an average of 2,423 assailable points down to 196 or an overall ***reduction by nearly 92%.***

With a pervasive model, SIL explored the risk of incursions and exposure using a blended measurement and emulation mechanism to test out new technology. The use of selective versus pervasive encryption showed that the combination of fewer manual tasks and the increased speed produced savings as much as ***81.63% less*** than x86.

Where today the security personnel load for IBM Z requires approximately ***80% less*** staff, the use of pervasive security will allow that staffing level to remain static while the alternate platforms will continue to grow - each year substantially.

Overall cost savings were also significantly different. The TCO for the same operating unit with pervasive versus selective encryption was ***only 36.7%*** of the overall IT budget. The impact on the organization as a whole is substantial, touching on a large number of areas, from line-of-business to application development.



While the IBM mainframe architecture can deliver individual transactions ***2.87-3.24 times faster***, the inclusion of the pervasive topology and approach increases that multiplier significantly. The underlying activity flow allows the pervasive model to deal with batches of transactions as a unit, rather than individual encryptions resulting in encryption that is ***18.4 times faster*** than alternate platforms. The resulting operational cost for pervasive encryption is ***5.1-8.0% of the cost*** of other options.

One area of interest was the subset of incursions that relied on the theft of encryption keys. The stolen information was part of the public and private pairing used in the industry to secure intra-platform activities. This exposure was completely eliminated by the hardware encryption model that is present in the Z solution. With no need for handshake pairing, there were no reported successful incursions in the 14-month window of the study.

Since the impact of the thefts of other encryption keys totaled more than $6,587,500 in the study timeframe, that safeguard is another substantial advantage for the pervasive security solution.

Recent Events

During the time of the SIL study, there were several significant events in the security world that are germane to the challenges addressed by encryption. A weaponized virus was set loose that mimicked a ransomware attack. In actuality, it was a weapon, made to destroy. The damage from this deliberate attack was comprehensive and considerable.

Governments, hospitals, airports, and businesses were targeted, attacked, and damaged. The costs on this are still being tabulated, and will probably continue for many years. The net impact, however, was that this type of attack can and will happen again. The type of encryption that this new advance represents would've stopped it since the ability to subvert the file control is a protected aspect of the encryption layer and would therefore not be vulnerable to hacking attacks.

The trillions of dollars in effects would have been saved and the people physically hurt, and businesses that have been negatively impacted would have been safe. This fundamental change in the security paradigm for the industry is profound.

At this point in time, no other chip architecture can support the pervasive encryption model. This is due to the technical limitations on bandwidth and overhead. It will be a challenge for those architectures to tool up and build out this capability, but it is one that the industry sorely needs.

Net Effects

The TCO of the encryption will require companies to look at their IT budgets. Since much of the IT budget is weighted toward application development, ***averaging 41.5-68.2%*** for the organizations within the study, any change that allows this to be reduced has an immediate effect on an organization's bottom line.

By moving encryption as a foundational security aspect to the center of a computing environment, the net effect on the IT budget would be a ***reduction of approximately 22.1%***.

"The implications of this mean that the cyberattack could be interpreted as an act of war, according to the organization. On Wednesday, NATO secretary general Jens Stoltenberg said a cyber attack could trigger Article 5, the principal of collective defense."

Luke Graham |@LukeWGraham, Friday, 30 Jun 2017 | 9:50 AM ET, Tech Transformers, A CNBC Special Report

---

Read full paper >

This document was developed with IBM funding. Although the document may utilize publicly available material from various vendors, including IBM, it does not necessarily reflect the positions of such vendors on the issues addressed in this document.

ID #66014266USEN-00